

في مايو 2021، تعرضت شركة Colonial Pipeline في الولايات المتحدة لهجوم إلكتروني بواسطة برمجية الفدية (ransomware). Colonial Pipeline هي شركة نقل وتوزيع الوقود تدير خط أنابيب يمتد على طول الساحل الشرقي للولايات المتحدة.

تم تنفيذ الهجوم بواسطة مجموعة إجرامية تعرف باسم "DarkSide"، وهي مجموعة قرصنة تستهدف المؤسسات وتشتهر بطلب فدية مالية مقابل فك تشفير البيانات المختطفة. تم اختراق نظام Colonial Pipeline وتشفير بياناتها، مما أدى إلى تعطيل عمليات النقل والتوزيع للوقود على طول الخط.

بمجرد تنفيذ الهجوم، قامت Colonial Pipeline بإيقاف تشغيل الخطوط البترولية للحيلولة دون انتشار البرمجية الخبيثة إلى المزيد من أجهزتها. استمر تعطيل عمليات النقل لعدة أيام، مما أثر على إمدادات الوقود في العديد من الولايات الشرقية في الولايات المتحدة وأدى إلى ارتفاع أسعار الوقود وشح في الإمدادات.

لحسن الحظ، تعاونت Colonial Pipeline مع السلطات الأمنية وشركات الأمان للتعامل مع الهجوم. قدمت الشركة فدية قدرها 4.4 مليون دولار للمجرمين الإلكترونيين للحصول على مفتاح فك التشفير الخاص ببياناتها المشفرة. وبالرغم من أن الفدية تم تسليمها، إلا أنه تمكنت السلطات من استعادة جزء كبير من الأموال المدفوعة بواسطة الشركة.

الهجوم على Colonial Pipeline أظهر التهديد المتنامي للبرمجيات الخبيثة والقرصنة الإلكترونية على البنية التحتية الحيوية للدولة والشركات. وقد أثار الحادث قلقًا كبيرًا حول أمن البنية التحتية الحيوية وأهمية تعزيز الأمان الإلكتروني وتعاون القطاع العام والخاص لمكافحة هذه الهجمات.